REMARKS

I. Initial Remarks

Claims 1-20 and 25-32 are pending, with claims 1, 6, 11 and 16 written in independent form. No claims are added, amended or canceled in this paper. In the Office Action, the Examiner maintained her rejections of claims 1-20 and 25-32 under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Pat. Pub. No. 2002/0184390 to Hasan Alkhatib ("Alkhatib"). The Examiner further included additional clarifications regarding the rejections of the claims. Applicants respectfully traverse the rejections, specifically responding to the additional clarifications by the Examiner. For at least the following reasons, all claims are in condition for allowance.

In view of the following arguments, all claims are believed to be in condition for allowance over the references of record. Therefore, this response is believed to be a complete response to the Office Action.[1] Further, for any instances in which the Examiner took Official Notice in the Office Action, Applicants expressly do not acquiesce to the taking of Official Notice, and respectfully request that the Examiner provide an affidavit to support the Official Notice taken in the next Office Action, as required by 37 CFR 1.104(d)(2) and MPEP § 2144.03.

II. Claim Rejections – 35 U.S.C. §102

MPEP § 2131 states that to anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "'The identical invention must be shown in as complete detail as is contained in the . . . claim.' See *Richardson v. Suzuki Motor Co.*, 868 F. 2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)." As detailed in the subsections below, each and every element as set forth in the claims is not found in Alkhatib. Therefore, for at least the following reasons, the Section 102(e) rejection of claims 1-20 and 25-32 should be withdrawn and the claims allowed.

[1] As Applicants' remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicants' silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references, assertions as to dependent claims, etc.) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicants reserve the right to analyze and dispute such assertions/requirements in the future.

A. Independent Claim 1

Independent claim 1 was rejected under Section 102(e) as allegedly being anticipated by Alkhatib. However, Alkhatib fails to anticipate at least (1) "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time;" (2) to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data;" (3) to "decrypt . . . to determine a restored address;" and (4) to "place the restored address back into the packet header information of the data packet," each as recited in the context of claim 1.

1. *"a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time"*

Independent claim 1 recites in part "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time." In the Office Action, paragraph 67 of Alkhatib was cited as allegedly disclosing these recitations. (Office Action, page 4.) While Alkhatib mentions "unencrypting," Alkhatib fails to anticipate "a key exchanger" at all, let alone "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited in the context of claim 1.

Alkhatib discloses a "data unit" addressed to a global address of a "domain name router," where the "data unit" additionally includes a "domain name." (e.g., Alkhatib, Abstract.) Alkhatib further discloses that "the Domain Name Router [(DNR)] receives the data, extracts the destination's domain name from the data, translates that domain name to a local address in its stub network and sends the data to the destination." (Alkhatib, paragraphs 12 and 14.) In Alkhatib, the "extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc." (Alkhatib, paragraph 36.)

Cited paragraph 67 is in reference to Figure 10 of Alkhatib, which discloses the steps "receive packet," "identify domain name," "translate," and "send data." As cited by the Examiner, "if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc." (Alkhatib, paragraph 67.) However, Alkhatib fails to disclose or suggest any details of the decode, decompress or unencrypt operations. Specifically, Alkhatib at least fails to anticipate "a key exchanger configured to repeatedly derive a cipher key," let alone "a

key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time," each as recited in the context of claim 1.

In response to previous arguments, the Examiner further stated that:

> Alkhatib provides for the encoding/translation of addresses in order to provide more efficient use of storage space, security and compatibility (par 36). This translation may be done via known methods of encryption, compression, or encoding and allows for an entity to secure data at one end while allowing for the receiving entity to extract the information at a later time by unencoding, decoding, decompressing, unencrypting the information using that same information that was used to encode, compress or encrypt the information originally.

(Office Action, page 2.) Paragraph 36 of Alkhatib discloses that "the source and destination's domain names are added to Options field 22" and that "the two domain names can be encoded, compressed, encrypted or otherwise altered to provide more efficient use of storage space, security or compatibility." (Alkhatib, paragraph 36.) The paragraph further states that:

> In embodiments where the domain name is encoded, encrypted, compressed, etc., the information stored is said to represent the domain name. That is, an entity can read that information and extract (or identify) the domain name from that information. That extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc.

(Id.) Rather than disclosing "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as expressly recited by claim 1, Alkhatib instead states in the most general terms that "extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc.," and "if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc." (Alkhatib, paragraphs 36 and 67.) For at least these reasons, Alkhatib fails to disclose "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited by claim 1.

Further, to the extent the Examiner is taking Official Notice regarding what "methods of encryption, compression, or encoding" are allegedly "known" within the context of the recitations of claim 1, the Examiner is hereby requested to provide support for such Official Notice in the next

response, as required by 37 CFR 1.104(d)(2). Such support must include both evidence sufficient to show "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited in the context of claim 1, as well as a proper rationale for how the supporting evidence would reasonably be combined with Alkhatib.

For at least these reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

2. *"decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data"*

Similar to as discussed above, while Alkhatib mentions only in the most general terms that "DNR 148 would need to decode, decompress, unencrypt, etc.," Alkhatib fails disclose any details at all of these decode, decompress, or unencrypt operations. In particular, Alkhatib fails to disclose or suggest "a cipher algorithm" and a "cipher key," let alone "a cipher algorithm keyed by the cipher key." Accordingly, Alkhatib fails to anticipate to "decrypt" any information "according to a cipher algorithm keyed by the cipher key," let alone to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" as recited within the context of the claim 1. This lack of disclosure is further evident when considered in the context of claim 1. Not only does Alkhatib fail to anticipate to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" but moreover, Alkhatib further fails to anticipate the recitations within the further context of "to repeatedly derive a cipher key such that the resulting cipher key changes over time" as recited in claim 1 and discussed above.

As indicated above, in response to previous arguments, the Examiner further stated that:

> Alkhatib provides for the encoding/translation of addresses in order to provide more efficient use of storage space, security and compatibility (par 36). This translation may be done via known methods of encryption, compression, or encoding and allows for an entity to secure data at one end while allowing for the receiving entity to extract the information at a later time by unencoding, decoding, decompressing, unencrypting the information using that same information that was used to encode, compress or encrypt the information originally.

(Office Action, page 2.) However, as discussed above and in the previous response, Alkhatib fails to disclose "a key exchanger configured to repeatedly derive a cipher key such that the resulting cipher key changes over time" and to "decrypt, according to a cipher algorithm keyed by the cipher key" as recited in the context of claim 1. Rather than disclosing these elements as expressly recited by claim 1, Alkhatib instead states only that "extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc.," and "if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc." (Alkhatib, paragraphs 36 and 67.) Moreover, the cited portions of Alkhatib do not support the assertion that the decoding is done "using that same information that was used to encode" as alleged in the Office Action.

To the extent that the Examiner is taking Official Notice that to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address" is allegedly "known" within the context of the recitations of claim 1, the Examiner is hereby requested to provide support for such Official Notice in response, as required by MPEP section 2144.03 and 37 CFR 1.104(d)(2), including a rationale how the additional support may reasonably be combined with Alkhatib.

For at least these reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

3. *"decrypt, . . . to determine a restored address"*

Independent claim 1 recites in part to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address," within the further context of "a translator configured to restore predetermined portions of packet header information of a data packet." In the Office Action, the Examiner cited paragraphs 12, 14, 36, and 67 of Alkhatib as allegedly disclosing the recitations. (Office Action, page 5.)

Alkhatib discloses to insert a "domain name" into the "Options Field 80" of a header or into a data portion 102 of a TCP segment. (Alkhatib, paragraph 48.) Using this inserted "domain name," Alkhatib further discloses to "[translate] that domain name to a local address and send the data to the destination [i.e., send to the translated local address]." (Alkhatib, Abstract.) In some

instances, "information used to represent the domain name could include an encrypted version of the domain name, an encoded version of the domain name, a compressed version of the domain name, etc." (Alkhatib, paragraph 14.) If so, "then DNR 148 would need to decode, decompress, unencrypt, etc." the information to retrieve the domain name. (Alkhatib, paragraph 67.)

While Alkhatib mentions generally that "DNR 148 would need to decode, decompress, unencrypt, etc.," Alkhatib fails to disclose that the data element that is being decoded, decompressed, or unencrypted is in fact a "restored address." Instead, Alkhatib discloses to "decode, decompress, [or] unencrypt" the inserted "information used to represent the domain name," not a "restored address." (Emphasis added.) Rather than being a "restored address" the decoded "domain name" is instead an input to the DNR that may be translated into "a local address" by the DNR. (Alkhatib, paragraph 52.)

Moreover, the "local address" of Alkhatib is also not a "restored address" as recited in the context of claim 1. As discussed above, the "local address" of Alkhatib is translated from the "domain name." However, the "local address" of Alkhatib is not a portion of an original packet created by the sender and put back into its original form. Accordingly, the "local address" of Alkhatib is not "a restored address" within the context of "a translator configured to restore predetermined portions of packet header information of a data packet" as recited by claim 1, let alone within the further context of to "decrypt . . . the extracted packet header data to determine a restored address" also as recited by claim 1.

For at least these additional reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

4. *"place the restored address back into the packet header information of the data packet"*

Independent claim 1 recites in part to "place the restored address back into the packet header information of the data packet." In the Office Action, the Examiner stated that:

> (par 12 "the Domain Name Router receives the data, extracts the destination's domain name from the data, translates that domain name to a local address in its stub network and sends the data to the destination; par 14; par 36 "That extraction or identification can be by unencoding, decoding, decompressing, unencrypting, etc"; par 67.)

(Office Action, page 5.) However, Alkhatib further fails to anticipate to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1.

Alkhatib discloses that an additional "domain name" data element that may be translated into a "local address." (See, Alkhatib, Abstract.) However, as discussed above, the "local address" of Alkhatib is not a portion of an original packet created by the sender and put back into its original form. Thus, not only does Alkhatib fail to anticipate to "decrypt . . . the extracted packet header data to determine a restored address" " as recited by claim 1, but Alkhatib further fails to anticipate "a restored address" within the context of to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1.

For at least these reasons, independent claim 1 and all claims that depend therefrom are patentable over Alkhatib.

B. Independent Claims 6, 11 And 16

Each of independent claims 1, 6, 11 and 16 was rejected under Section 102(e) as allegedly being anticipated by Alkhatib. While claims 1, 6, 11 and 16 are each of different scope, for at least reasons similar to those discussed above with regard to independent claim 1, independent claims 6, 11, and 16 are patentable over Alkhatib.

For example, as discussed above with regard to independent claim 1, Alkhatib does not teach or suggest "to repeatedly derive a cipher key such that the resulting cipher key changes over time," to "decrypt, according to a cipher algorithm keyed by the cipher key, the extracted packet header data to determine a restored address," and to "place the restored address back into the packet header information of the data packet" as recited in the context of claim 1. Independent claims 6, 11, and 16 each includes like recitations, although claim 6 recites "decrypting" and "placing," claim 11 recites "means for repeatedly deriving," "means for decrypting," and "means for placing," and claim 16 recites to "repeatedly derive."

Accordingly, for at least similar reasons to those discussed above with regard to independent claim 1, independent claims 6, 11, and 16 and all claims that depend therefrom are patentable over Alkhatib.

C. Dependent Claims 2-5, 7-10, 12-15 And 25-32

Claims 2-5, 7-10, 12-15, and 25-32 are in condition for allowance at least because they depend from one of independent claims 1, 6, 11, or 16. Further, the dependent claims also recite independently patentable subject matter, representative examples of which are discussed below.

1. Claim 25

Claim 25 depends from independent claim 1 and recites in part "the host portion of the address having been translated without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address." In the Office Action, the Examiner cited paragraph 67 of Alkhatib as allegedly disclosing the recitations, without explanation. (Office Action, page 6.)

Paragraph 67 of Alkhatib discloses in part that:

> FIG. 10 describes the steps performed by DNR 138 when it receives the IP packet from host 150. In step 502, DNR 138 receives the IP packet. In step 504, DNR 138 identifies the destination's domain name from the packet. Identifying the domain name could include looking for the domain name in the header, data portion or other location in an IP packet, TCP segment, application data, etc. Identifying the domain name may include reading an ASCII string. Alternatively, if the domain names are compressed, encrypted, encoded, etc., then DNR 148 would need to decode, decompress, unencrypt, etc. In step 506, DNR 138 translates the destination domain name to a local address and in step 508 the packet is routed to the destination with the local address.

(Alkhatib, paragraph 67.) Alkhatib further discloses that "the global address for DNR 138 in the IP packet is replaced with the local address in the table" and "the checksum for the IP header is adjusted if necessary." (Alkhatib, paragraph 68.) Moreover, as cited earlier in the Office Action, paragraph 15 of Alkhatib states that:

> In one embodiment, the data unit sent to the Domain Name Router includes a global IP address for the Domain Name Router. After translating the domain name to a local address, the Domain Name Router will replace the global address for the Domain Name Router with the local address of the destination. The step of replacing the global address with the local address can include adjusting any appropriate checksums or any other necessary fields in the data unit.

(Alkhatib, paragraph 15; Emphasis added.) Thus, Alkhatib specifically discloses to overwrite the entire destination address of the data unit.

Because Alkhatib discloses to overwrite the entire destination address of the data unit with "the local address of the destination," Alkhatib accordingly replaces both the network portion of the destination address and also the host portion of the destination address. Thus, as Alkhatib replaces the entire destination address, Alkhatib fails to anticipate "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address." (Emphasis added.) For at least these reasons, claim 25 is separately patentable over Alkhatib.

In response to previous arguments, the Examiner stated that:

> Alkhatib provides for a variety of embodiments whereby different portions of a packet's address may be translated while others remain untranslated and whereby different portions of the addresses may be placed in different areas of the headers (par 56). For example, in paragraph 67 the situation arises in which the routing and translation serves to transport the packet to a secondary location where yet another translation must be done in order to locate a particular address within a larger address space.

(Office Action, page 3.) Applicants respectfully disagree that Alkhatib provides that "different portions of a packet's address may be translated while others remain untranslated." Rather, Alkhatib discloses only that a "domain name" is translated into a "local address," not "different portions of a packet's address." (See Alkhatib, Abstract, Fig. 10, paragraphs 12, 15, 52 and 67, and claims 1, 21 and 41.) Moreover, paragraphs 56 and 67 of Alkhatib fail to cure the aforementioned deficiencies of Alkhatib with respect to "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25.

Cited paragraph 56 discloses that "FIGS. 7-10 are flow charts which describe the process for sending data according to the present invention." (Alkhatib, paragraph 56.) The paragraph then discusses aspects of the hosts, and states that: "a message is being sent from host 150 to host 132," "host 132 has a local address and host 150 has a global address," "it is assumed that host 150 and 132 are computers," and "host 150 and 152 can be other electronic devices." (Id.) However such a disclosure does not bear any relation to "the host portion of the address having been translated

without the network portion also being translated, and wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25.

As discussed above, the translation disclosed in Alkhatib overwrites the entire destination address of the data unit. Thus, regardless of how many translations of the type disclosed in Alkhatib are performed, the translation in Alkhatib does not anticipate "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited in the context of claim 25. Paragraph 67 discloses in relevant part that:

> FIG. 11 describes one exemplar embodiment for performing the step of translating the destination domain name to a local address (step 506 of FIG. 10). Other suitable methods of translating a domain name can also be used. Translating a domain name can include less than all of the steps of FIG. 11. In step 512, DNR 138 looks up the domain name in a DNR table stored in its memory or other storage device. The DNR table includes domain names and corresponding local addresses. In one embodiment, the DNR table could also include Ethernet addresses. It is also possible that the local network includes multiple DNRs, forming a tree. Thus, the entry in the DNR table for a particular domain name could be just an address for another DNR. The packet would then be sent to another DNR, and the second DNR that would then use the domain name to find the final (or next) local address to the destination or another DNR, etc. The DNR table can be set up manually by the administrator for the network or may be set up automatically through embedded software, firmware or hardware.

(Alkhatib, paragraph 67.) While Alkhatib discloses that a "packet would then be sent to another DNR, and the second DNR that would then use the domain name to find the final (or next) local address to the destination or another DNR," such disclosure bears no relation to "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited by claim 25. In contrast, each forward to a next DNR overwrites the entire destination address of the data unit. Overwriting the destination address multiple times, however, does not teach or suggest "wherein said translator is configured to restore the host portion of the address without also restoring the network portion of the address" as recited in the context of claim 25.

Accordingly, at least for the reasons discussed above and in previous papers, claim 25 is separately patentable over Alkhatib.

2. Claims 27, 29 And 31

Claims 27, 29 and 31 were rejected under Section 102(e) as allegedly being anticipated by Alkhatib. (Office Action, pages 6-7.) As discussed above with regard to claim 25, Alkhatib does not teach or suggest "to restore the host portion of the address without also restoring the network portion of the address." Claims 27, 29, and 31 depend from different base claims, but each includes like recitation. Thus, while claims 25, 27, 29, and 31 are each of different scope, for at least reasons similar to those discussed above with regard to claim 25, claims 27, 29, and 31 are separately patentable over Alkhatib.

III. CONCLUSION

In view of the above remarks, the pending application is in condition for allowance. Reconsideration and allowance are respectfully requested.

It is believed that any fees associated with the filing of this paper are identified in an accompanying transmittal. However, if any additional fees are required, they may be charged to Deposit Account No. 18-0013, under Order No. 65632-0534. To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged against the aforementioned account.

Dated: December 7, 2010

Respectfully submitted,

Electronic signature: /Isaac T. Slutsky/
Michael B. Stewart
Registration No.: 36,018
Isaac T. Slutsky
Registration No.: 64,620
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorneys for Applicants